Registering Apps(version 1.0)

**Cloud Service Label:  IaaS, PaaS**

Description

Adversaries can utilize cloud app stores to create malicious applications that request permissions to sensitive data. These applications would appear as legitimate to users which could lead to users granting the requested permissions. This is similar to downloading malicious applications on a computer or cellular device. The data exposed to adversaries utilizing this technique can lead to initial access, persistence, and privilege escalation.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Microsoft (illicit consent grant attack) | Microsoft outlines how an adversary would first register an app with a provider, such as Azure Active Directory. Then an attacker will use that to send an email to users as a “legitimate” request to authenticate which will prompt for the user to grant permissions to the malicious app. It will then have access to information such as mail, forwarding rules, files, contacts, notes, profile, and other information. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Approved Applications Only | Users should only be allowed to install company allowed applications. The applications installed by users should be audited frequently to assure no malicious applications are installed. |

Detection

This can be difficult to detect due to the fact that users are granting permissions to what is seen as a legitimate application.

References

1. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide. Accessed July 16, 2020.